Anti Piracy K&T Discussion

E. Kwon
NTD / 15-April-2013

Summary

- Latest CTR NUP has fixed some code-injection invulnerabilities.
- CTR hacking efforts seem to be slowed down.
- Questions from NCL:
  - Should we stop Neimod Knock and Talk?
  - Should we switch target? (Yellows8)

Neimod Knock and Talk

- We should proceed.
- Rationale:
  - Neimod hacking efforts are maybe delayed, not stopped by NUP fixes.
    - *Hackers are suspicious that Nintendo is aware of their activities, and may be more cautious to discuss on internet.*
  - Neimod has invested significant time and energy to build FPGA-based “ramhax”.
  - Neimod can still use older firmware to seek other exploits.

Should We Change Target?

- We should consider additional targets.
- Rationale:
  - Capturing individual hackers is NOT the goal.
  - **Changing the opinion of hackers about Nintendo is the goal.**
  - Many hackers think Nintendo is “safe” (never pursues hackers)
  - Many hackers are hacking other platforms, but NOT releasing exploits, because of bounties/rewards.

Should We Pursue Yellows8

- Actually, no. Not at this time.
- Rationale:
  - Not enough information about Yellows8.
  - One of the key reasons we select Neimod is because we can predict a reasonably good chance for success.
  - Lack of knowledge about Yellows8 means risk for negative outcome is very high.

Emphasis: Hearts and Minds

- Reacting to individual hackers is dangerous and never-ending.
  - Some hackers may be completely silent (no public profile).
  - As we pursue hackers, open discussion on the internet may cease.
- Hackers can work for Nintendo
  - If hackers believe Nintendo is friendly, hackers are much more likely to submit exploits to us.
  - If we K&T certain hackers, the hacker community will likely work with them (i.e., Neimod).

Supporting Material

Intel re: Hacking Eco-System

- ICG Logs - “bob_” is confirmed to be “geohot”

```
[2013/03/17 20:01:24] <blasty> yo egohot
[2013/03/17 20:01:55] <blasty> won 70k with readeR?
[2013/03/17 20:02:57] <blasty> 0day soldier of fortune
[2013/03/17 20:03:12] <blasty> I hear ZDI doesnt buy 3ds browser bugs th0
```

IRC user asks geohot (“bob_”) if he won $70,000 USD for discovering Adobe Acrobat exploit.

Implies hackers are making money from discovery of zero-day exploits.

No way for hackers to make money from discovering Nintendo vulnerabilities.

```
[2013/03/17 20:07:58] <bob_>   (well marketed, you'll make the same on jailbreak
                               donations)
[2013/03/17 20:08:15] <blasty> lol
[2013/03/17 20:08:39] <blasty> don't expect any such quantity of donations for
                               hacking a stupid nintendo console

[2013/03/17 20:52:38] <neimod> just make sure you're legally covered before you
                               start to release anything :P
[2013/03/17 20:53:11] <bob_>   i'd be surprised if i got sued again
[2013/03/17 20:53:29] <bob_>   but always :P
[2013/03/17 20:53:48] <bob_>   (or just don't release)
```